Számelmélet és valószínűségszámítás

Rátz László Vándorgyűlés

2021. július 3.

Freud Róbert

freudro8@gmail.com

A Csebisev-egyenlőtlenség két számelméleti alkalmazását mutatjuk be, amelyek specmaton vagy erős szakkörön is tárgyalhatók. Az egyik Erdős Pál egy kedvenc problémájához kapcsolódik, a másik pedig Turán Pál egyszerű bizonyítása Hardy és Ramanujan híres tételére.

Mindkettő elmondható valószínűségszámítás nélkül is, de éppen a valószínűségi szemlélet mutatja meg a lényeget.

1. Csebisev-egyenlőtlenség (1867)

Informálisan: Egy valószínűségi változó nagy valószínűséggel a várható értékétől nem túl távoli értéket vesz fel. Itt a távolság „egysége” a szórás.

Pontosan: Ha a ξ valószínűségi változó várható értéke E és szórása D, akkor tetszőleges $c > 0$-ra

$$P(|\xi - E| > cD) < \frac{1}{c^2}.$$

Ezt csak a legegyszerűbb, klasszikus valószínűségi mezőre fogjuk alkalmazni, amikor ξ a $v_1, v_2, \ldots, v_N$ értékek mindegyikét $1/N$ valószínűséggel veszi fel. Ennek a speciális esetnek a bizonyítása középiskolában is könnyen elmondható.

$$E = \frac{v_1 + v_2 + \ldots + v_N}{N} \text{ és } D = \sqrt{\frac{(v_1 - E)^2 + \ldots + (v_N - E)^2}{N}},$$

azaz $NE = \sum_{i=1}^{N} v_i$ és $ND^2 = \sum_{i=1}^{N} (v_i - E)^2$.

Legyen s, ahányszor $|v_i - E| > cD$. Be kell látni, hogy $s/N < 1/c^2$.

$$ND^2 = \sum_{i=1}^{N} (v_i - E)^2 > \sum_{|v_i - E| > cD} (v_i - E)^2 > s(cD)^2, \text{ így } N > c^2 s.$$

2. Csupa különböző összeg

Erdős Pál egyik kedvenc problémája: Maximálisan hány pozitív egész adható meg n-ig, hogy közülük akárhány különbözőt összeadva (beleértve az egytagú összegeket és az összes szám összegét is) mindig különböző számot kapunk?

Azaz $1 \leq a_1 < a_2 < \ldots < a_k \leq n$, minden részösszeg különböző, mennyi a k maximuma (n függvényében)?

Ilyenek például a 2-hatványok, tehát $\max k \geq 1 + \lfloor \log_2 n \rfloor > \log_2 n$.

Felső becslés: Megnézzük, hány részösszeg van és ezek milyen intervallumba eshetnek. Mivel minden részösszeg különböző egész szám, ezért legfeljebb annyi részösszeg lehet, mint amennyi az intervallum hossza.

A részösszegek száma $2^k - 1$. Mindegyik legalább 1 és legfeljebb

$$n + (n-1) + \ldots + (n-k+1) \leq nk - 1.$$

Minden részösszeg különböző, tehát $2^k - 1$ egésznek el kell férnie 1 és $nk - 1$ között. Ezért

$2^k - 1 \leq nk - 1$, azaz $2^k \leq nk$.

$$2^k \leq nk.$$

Logaritmálva:

$$(*)\ k \leq \log_2 n + \log_2 k \leq 2 \log_2 n.$$

Ezt is logaritmálva:

$$(**)\ \log_2 k \leq 1 + \log_2 \log_2 n.$$

(**)-ot beírva (*)-ba:

$$k \leq \log_2 n + \log_2 \log_2 n + 1.$$

Tehát

$$\log_2 n < \max k < \log_2 n + \log_2 \log_2 n + 1.$$

$$1 < \frac{\max k}{\log_2 n} < 1 + \frac{\log_2 \log_2 n + 1}{\log_2 n}.$$

$\lim_{n\to\infty} \frac{\max k}{\log_2 n} = 1$, azaz $\max k$ aszimptotikusan egyenlő $\log_2 n$-nel.

Erdős 500$: Igaz-e, hogy $|\max k - \log_2 n|$ korlátos?

Megjegyzés: Van a kettőhatványoknál eggyel(!) sűrűbb konstrukció, ha $n \geq 2^{21}$.

A $\log_2 \log_2 n$-es hibatagot meg tudjuk felezni a Csebisev-egyenlőtlenséggel, ugyanis az összegek az $[1, nk-1]$ intervallumban nem egyenletesen oszlanak el, hanem az átlag közelében sűrűbben helyezkednek el.

Legyen ξ az a valószínűségi változó, amelyik minden részösszeget (beleértve az üreset is) $1/2^k$ valószínűséggel vesz fel.

Ez azt jelenti, hogy ξ egymástól függetlenül 1/2–1/2 valószínűséggel teszi be az összegbe az egyes a_j-ket. Eszerint ξ az $\eta_1, \ldots, \eta_k$ független valószínűségi változók összege, ahol η_j a 0 és a_j értékeket veszi fel 1/2–1/2 valószínűséggel: $\xi = \sum_{j=1}^{k} \eta_j$.

Itt $E(\eta_j) = \dfrac{a_j}{2}$ és $D^2(\eta_j) = \left(\dfrac{a_j}{2}\right)^2$.

Ekkor $E(\xi) = \sum_{j=1}^{k} E(\eta_j) = \sum_{j=1}^{k} \frac{a_j}{2}$.

Ugyanez közvetlenül is adódik, ha minden részösszeget a komplementerével összepárosítunk, hf.

Szórás: $D^2(\xi) = \sum_{j=1}^{k} D^2(\eta_j) = \sum_{j=1}^{k} \left(\frac{a_j}{2}\right)^2 < \frac{kn^2}{4}$.

Ez is megy közvetlenül, hf.

Tehát $D(\xi) < n\sqrt{k}/2$.

Csebisev pl. $c = 2$-vel: Az átlagtól a szórás kétszeresénél távolabb eső összegek száma kevesebb, mint az összes összeg számának a negyedrésze.

Tehát több, mint $2^k \cdot \frac{3}{4}$ összeg esik egy $4D(\xi) = 2n\sqrt{k}$ hosszúságú intervallumba, amelynek a középpontja $E(\xi)$.

Ezek az összegek mind különbözők, így

$$2^k \cdot \frac{3}{4} < 2n\sqrt{k}, \qquad \text{azaz} \qquad 2^k < \frac{8n\sqrt{k}}{3}.$$

Ezt a korábbihoz hasonlóan kétszer logaritmálva kapjuk, hogy

$$k < \log_2 n + \frac{\log_2 \log_2 n}{2} + 2.$$

További érdekességek: Freud–Gyarmati: Számelmélet 12.1.

3. Tipikusan kb. hány prímosztója van egy számnak?

(Vázlat. Részletek: Számelmélet könyv 6.7.)

Legyen $\omega(n)$ az n pozitív egész különböző prímosztóinak száma. Pl. $\omega(20) = 2, \omega(64) = 1$.

Kb. mekkora az $\omega(n)$ az n függvényében?

Végtelen sok n-re, a prímhatványokra $\omega(n) = 1$.

De bármilyen nagy is lehet: az első s prím szorzatára $\omega(n) = s$, pl.

$$\omega(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19) = \omega(9699690) = 8.$$

Nem nagyon látszik semmi szabályosság.

Belátjuk, hogy egy jól ismert, „szép” $f(n)$ függvénnyel mégis teljesül, hogy a legtöbb számra $\omega(n)$ kb. $f(n)$. A „legtöbb” és „kb.” kifejezések persze pontos matematikai tartalmat jelentenek.

Legyen t egy tetszőleges (nagy) pozitív egész. Először kiszámítjuk, hogy $\omega(n)$ átlagosan mekkora 1 és t között:

$$E = \frac{\omega(1) + \omega(2) + \ldots + \omega(t)}{t} = \frac{W(t)}{t}.$$

$$E = \frac{\omega(1) + \omega(2) + \ldots + \omega(t)}{t} = \frac{W(t)}{t}.$$

$W(t)$ becsléséhez tekintsük azt a $t \times t$-es mátrixot, amelynek az i-edik sorában az $\omega(i)$-t „számoljuk meg”, azaz minden j-edik helyre 1-et írunk, ahol a j az i valamelyik prímosztója, a többi helyre pedig 0 kerül. Pl. $t = 6$-ra:

	1	2	3	4	5	6
$\omega(1) = 0$	0	0	0	0	0	0
$\omega(2) = 1$	0	1	0	0	0	0
$\omega(3) = 1$	0	0	1	0	0	0
$\omega(4) = 1$	0	1	0	0	0	0
$\omega(5) = 1$	0	0	0	0	1	0
$\omega(6) = 2$	0	1	1	0	0	0

Tehát az i-edik sor j-edik eleme 1, ha j prímszám és osztója i-nek, egyébként pedig 0.

Hány 1-es van a mátrixban?

Soronként összegezve $\sum_{i=1}^{t} \omega(i) = W(t)$.

Ha $j = p$ prímszám, akkor a p-edik oszlopban a p többszöröseinek megfelelő helyeken áll 1, tehát itt $\lfloor t/p \rfloor$ darab 1-es van, minden más elem 0. Így oszloponként összegezve az 1-esek száma $\sum_{p \le t} \left\lfloor \frac{t}{p} \right\rfloor$, ahol az összegzés csak a prímekre történik. A továbbiakban p, q mindig prímszámot jelöl.

Tehát $W(t) = \sum_{p \le t} \left\lfloor \frac{t}{p} \right\rfloor$.

Vagyis az $\omega(n)$ átlaga $1 \le n \le t$-re

$$E = \frac{W(t)}{t} = \frac{1}{t} \sum_{p \le t} \left\lfloor \frac{t}{p} \right\rfloor = \left(\sum_{p \le t} \frac{1}{p} \right) - h(t), \text{ ahol } 0 \le h(t) < 1.$$

Mivel a prímek reciprokösszege t-ig kb. $\ln \ln t$, ezért az $\omega(n)$ átlagosan kb. ennyi. Vagyis egy 1 és t közötti egésznek átlagosan $\ln \ln t$ különböző prímosztója van. Pl. $t = 10^{100}$-ra ez $5{,}44$.

Az $\ln \ln x$ függvény nagyon lassan növekszik. Pl. $\ln \ln \sqrt{t} = \ln(\ln t/2) = \ln \ln t - \ln 2$, ezért $\sqrt{t}$ és t között csak $\ln 2$ a növekedés. Ezért az 1 és t közötti „majdnem minden” n esetén „kb. $\ln \ln t$” helyett nyugodtan mondhatunk „kb. $\ln \ln n$”-et is.

Abból azonban, hogy $\ln\ln n$ az átlag, nem következik, hogy a legtöbb esetben ehhez közeli a függvényérték, lehetnének nagy ingadozások és úgy jön ki ez az átlag. Hardy és Ramanujan bonyolult módszerekkel belátták (1917), hogy nem így van, a „legtöbb" n számnak tényleg kb. $\ln\ln n$ prímosztója van.

Turán Pál adott erre egy egyszerű bizonyítást (1934), amiben tulajdonképpen a Csebisev-egyenlőtlenséget használta (anélkül, hogy ennek tudatában lett volna), és ez lett a kiindulópontja a valószínűségszámítás számelméleti alkalmazásainak.

Legyen ξ az a valószínűségi változó, amelyik az $\omega(1),\dots,\omega(t)$ értékek mindegyikét $1/t$ valószínűséggel veszi fel. Ekkor ennek $E \approx \ln\ln t$ várható értékét számoltuk ki. Belátjuk, hogy kicsi a szórás, kisebb, mint $\sqrt{3E}$. Ekkor a Csebisev-egyenlőtlenség szerint ξ-nek E-től való eltérése nagy valószínűséggel $\sqrt{E}$ egy konstansszorosánál kisebb, azaz valóban majdnem minden n-nek kb. $\ln\ln n$ különböző prímosztója van.

A szórás kiszámítása heurisztikusan (Gyenes Zoltán javaslata):

A ξ változót fel tudjuk bontani prímenkénti indikátorváltozók összegére. Legyen p prím és κ_p értéke $1/p$ valószínűséggel 1 („a szám osztható p-vel”) és $(p-1)/p$ valószínűséggel 0 („a szám nem osztható p-vel”). Ekkor $\xi = \sum_{p \le t} \kappa_p$.

Az összes pozitív egészre nézve a κ_p változók függetlenek. Ugyanis a különböző prímekkel való oszthatóságok a páronként relatív prímség miatt egymástól függetlenek. Formálisan: a p-vel való oszthatóság valószínűsége $1/p$ és a $p_1, \ldots, p_r$ prímek mindegyikével való oszthatóság ugyanaz, mint a $N = p_1 \cdot \ldots \cdot p_r$ szorzattal való oszthatóság, tehát ennek a valószínűsége $1/N$, ami valóban az $1/p_i$ valószínűségek szorzata.

$$\xi = \sum_p \kappa_p; \quad \kappa_p = 1 \text{ valószínűsége } 1,\ \kappa_p = 0 \text{ valószínűsége } 0.$$

$$E(\kappa_p) = \frac{1}{p} \quad \text{és} \quad D^2(\kappa_p) = \frac{1}{p}\left(\frac{p-1}{p}\right)^2 + \frac{p-1}{p}\left(\frac{1}{p}\right)^2 = \frac{1}{p} - \frac{1}{p^2}.$$

„Kicsit” csalva tekintsük úgy, hogy a κ_p változók elég nagy t-re az 1 és t közötti egészekre szorítkozva is függetlenek maradnak. Ekkor

$$D^2(\xi) = \sum_{p \le t} D^2(\kappa_p) = \sum_{p \le t} \frac{1}{p} - \sum_{p \le t} \frac{1}{p^2} \approx E.$$

A szórás pontosan: $D^2(\xi) = E\big((\xi - E)^2\big) = E(\xi^2) - E^2$.

$$E(\xi^2) = \frac{1}{t}\sum_{i=1}^{t}\omega^2(i) = \frac{1}{t}\sum_{i=1}^{t}\omega(i)\sum_{p|i}1 = \frac{1}{t}\sum_{p\le t}\sum_{p|i}\omega(i) =$$

$$= \frac{1}{t}\sum_{p\le t}\sum_{v\le t/p}\omega(vp) \le \frac{1}{t}\sum_{p\le t}\sum_{v\le t/p}\big(1+\omega(v)\big) =$$

$$= \frac{1}{t}\sum_{p\le t}\left\lfloor\frac{t}{p}\right\rfloor + \frac{1}{t}\sum_{p\le t}\sum_{v\le t/p}\omega(v).$$

Az egyenlő(tlen)ségek magyarázata rendre: definíció — az (egyik) $\omega(i)$-re beírjuk a definíciót — összegátrendezés — oszthatóság átírása — egy számot egy prímszámmal szorozva legfeljebb eggyel nő a prímosztók száma — szétvágjuk az összeget két részre.

$$E(\xi^2) \le \frac{1}{t}\sum_{p\le t}\left\lfloor\frac{t}{p}\right\rfloor + \frac{1}{t}\sum_{p\le t}\sum_{v\le t/p}\omega(v).$$

Az első tag E. A második tag második szummája az átlagértéknél látottak szerint

$$\sum_{v\le t/p}\omega(v) = \sum_{q\le t/p}\left\lfloor\frac{\lfloor\frac{t}{p}\rfloor}{q}\right\rfloor < \sum_{q\le t/p}\frac{t}{pq} < \frac{t}{p}\sum_{q\le t}\frac{1}{q}.$$

Tehát a teljes második tag kisebb, mint

$$\left(\sum_{p\le t}\frac{1}{p}\right)^2 = \big(E+h(t)\big)^2 = E^2+2h(t)E+h^2(t) < E^2+2E.$$

Így $E(\xi^2) < E^2+3E$ és $D^2 = E(\xi^2)-E^2(\xi) < E^2+3E-E^2 = 3E$.